

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10066157 A**

(43) Date of publication of application: **06 . 03 . 98**

(51) Int. Cl.

H04Q 7/38

H04L 9/08

H04L 9/18

H04L 12/56

(21) Application number: **09149370**

(22) Date of filing: **06 . 06 . 97**

(30) Priority: **06 . 06 . 96 FI 96 962352**

(71) Applicant: **NOKIA MOBILE PHONES LTD**

(72) Inventor:
KARPPANEN ARTO
KARI HANNU
HAEMAELEINEN JARI
JUOPPERI JARI

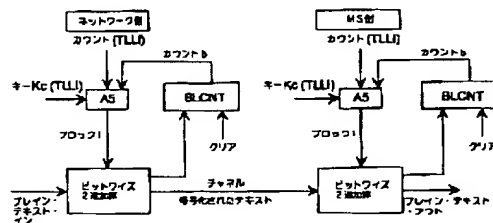
(54) INFORMATION-CIPHERING METHOD AND DATA COMMUNICATION SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To transfer data by mode of not ciphering a header field in a physical layer by dividing into function layers in which data transferring systems are different at each layer of different data frame structure.

SOLUTION: A not ciphered sub-block (plain text in) is ciphered from a network side and transferred to a mobile station (MS) side as a ciphered block (ciphered text). A block counter (BLCNT) is set to be an initial value by a set line signal (clear) at the time of starting a data frame of each adaptive layer and generates a data count (count (b)). A ciphering algorithm A8 calculates an output bit string (block 1) for each block from a prescribed ciphering key Kc and the count (b). A network side obtains a text by bit-adding a block 1 to the plain text.

COPYRIGHT: (C)1998,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-66157

(43) 公開日 平成10年(1998) 3月6日

(51)Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所	
H 0 4 Q	7/38		H 0 4 B	7/26	1 0 9 R
H 0 4 L	9/08		H 0 4 L	9/00	6 0 1 C
	9/18				6 5 1
	12/56	9744-5K		11/20	1 0 2 Z

審査請求 未請求 請求項の数20 O L (全 12 頁)

(21) 出願番号 特願平9-149370

(22) 出願日 平成9年(1997) 6月6日

(31) 優先権主張番号 9 6 2 3 5 2

(32) 優先日 1996年6月6日

(33) 優先権主張国 フィンランド (F I)

(71) 出願人 590005612

ノキア モービル フォーンズ リミティ
ドフィンランド国、エフアイエヌ-02150
エスボー、ケイララーデンティエ 4

(72) 発明者 アルト カルパネン

フィンランド国、エフイーエン-00210
ヘルシンキ、ベチュニエメンカトゥ 4
デー 64

(72) 発明者 ハンヌ カリ

フィンランド国、エフイーエン-02880
ペッコラ、クラボンキヤ 9 ベー 9

(74) 代理人 弁理士 石田 敬 (外3名)

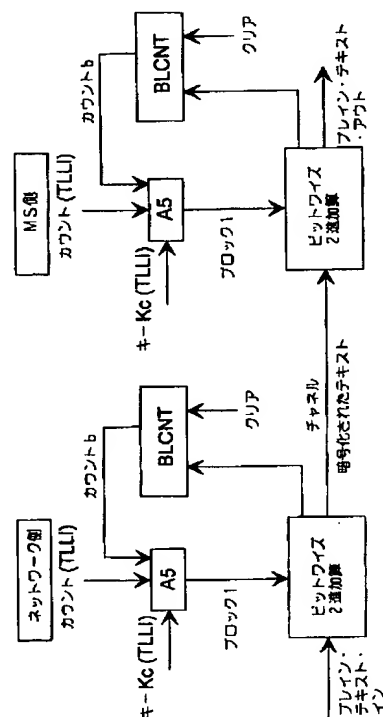
最終頁に続く

(54) 【発明の名称】 情報の暗号化方法およびデータ通信システム

(57) 【要約】

【課題】 転送されたデータがデータ・フレーム・モードにありかつデータ転送システムがデータ・フレーム構造が異なる層において異なることができるような機能層に分割されているデータ転送システムにおけるデータ転送の暗号化方法及び装置を提供する。

【解決手段】 一つ以上のデータ・フレームがアプリケーションによる情報から形成された一つ以上のデータ・パケットから生成されるデータ通信システムのデータ転送機器 (MS, SGSN) 間で転送された情報の暗号化方法が提供される。データ・フレームは、少なくともヘッダ・フィールド及びデータ・フィールドを含む。データ・パケットの少なくともある部分は、暗号化キー (Kc) を用いて暗号化される。データ・フレームに対して、同期データ (COUNT) が配属され、その値は、少なくとも各データ・フレームの伝送時に変えられる。



【特許請求の範囲】

【請求項1】 アプリケーションによって情報から形成された一つ以上のデータ・パケットから一つ以上のデータ・フレームが生成され、かつこれらのデータ・フレームは、少なくともヘッダ・フィールド及びデータ・フィールドを含む、データ通信システムのデータ転送機器（MS，SGSN）間で転送された情報の暗号化方法において、前記データ・パケットの少なくとも一つの部分は、暗号化キー（Kc）を用いて暗号化されかつ同期データ（COUNT）は、データ・フレームに配属されかつその値は、少なくとも各データ・フレームの伝送時に

【請求項2】 データ転送接続は、前記データ通信システムに接続された二つ以上のデータ転送機器（MS，SGSN）間で形成される前記方法において、個別の暗号化キー（Kc）が各接続に割り当てられ、同じデータ転送チャンネルで、少なくとも二つの個別接続のデータ・フレームは、互いに独立に暗号化モードで転送することができることを特徴とする請求項1に記載の方法。

【請求項3】 前記データ・フレームは、少なくとも一つのサブブロックに分割される前記方法において、前記同期データは、各接続に個別に割り当てられかつ初期値が接続の開始で設定されかつその値が各サブブロックの伝送時に変えられるブロック・カウンタ（BLCNT）を含むことを特徴とする請求項1または2に記載の方法。

【請求項4】 前記データ・フレームは、適応層（LLC）で形成されることを特徴とする請求項1，2または3に記載の方法。

【請求項5】 前記適応層の前記データ・フレームは、リンク層（MAC，RLC，LLC，L2）に転送され、前記リンク層のデータ・フレームは、伝送経路（Um，Gb）への伝送のための前記適応層の前記データ・フレームから形成されることを特徴とする請求項4に記載の方法。

【請求項6】 前記同期データ（COUNT）は、次の少なくとも一つ：

- 前記リンク層のデータ・フレーム番号（LLC#）、
- 前記適応層のデータ・フレーム番号（SDU#）、
- ルーティング・エリアの識別子（ルーティング・エリア#）、
- パケット・スイッチング・コントローラのエリアの識別子（SGSN#）、
- セルの識別子（Cell#）

を含むことを特徴とする請求項5に記載の方法。

【請求項7】 前記データ・フレーム番号（SDU#）は、データ転送接続に結合されたデータ転送機器（MS，SGSN）において形成されかつ局所的に維持され、シーケンス番号は、接続の開始でその初期値に設定

されかつそれは、接続の間に予め定義された方法で更新されることを特徴とする請求項6に記載の方法。

【請求項8】 前記リンク層のデータ・フレーム番号（LLC#）は、前記データ転送接続の一つのデータ転送機器（MS，SGSN）に維持されかつそれは、前記リンク層の前記データ・フレームにおける他のデータ転送機器に送付されることを特徴とする請求項6に記載の方法。

【請求項9】 前記データ転送接続は、GPRSシステムのような、パケット・スイッチング・システムのデータ転送接続であることを特徴とする請求項1から8のいずれか一項に記載の方法。

【請求項10】 前記データ転送接続は、ポイントツーポイント接続（PTP）であることを特徴とする請求項1から9のいずれか一項に記載の方法。

【請求項11】 前記データ転送接続は、ポイントツーマルチポイントマルチキャスト（PTM-M）またはポイントツーマルチポイントグループ（PTM-G）のような、マルチポイント接続であることを特徴とする請求項1から9のいずれか一項に記載の方法。

【請求項12】 情報は、データ・サービス・プロバイダの前記データ転送機器（SGSN）とデータ・サービス・ユーザの前記データ転送機器（MS）の間に転送され、各接続に個別に割り当てられた暗号化キー（Kc）は、前記データ転送機器のキーパッドまたはスマート・カード（SIM）を用いて、前記データ転送システムの暗号化モードで暗号化キー（Kc）を転送することによって前記データ転送機器（MS，SGSN）に設定されることを特徴とする請求項11に記載の方法。

【請求項13】 — 前記データ・サービス・プロバイダの前記データ転送機器（SGSN）から前記データ・サービス・ユーザの前記データ転送機器（MS）へ伝送されたデータだけが少なくとも部分的に暗号化され、
— 前記データ・サービス・ユーザの前記データ転送機器（MS）から前記データ・サービス・プロバイダの前記データ転送機器（SGSN）に伝送されたデータだけが少なくとも部分的に暗号化され、または、
— 両方の方向に伝送されたデータが少なくともある程度暗号化されることを特徴とする請求項11または12に記載の方法。

【請求項14】 暗号化の開始で、データ転送が暗号化される方向を考慮しているデータは、データ転送機器へ伝送されることを特徴とする請求項13に記載の方法。

【請求項15】 前記適応層の前記データ・フレームのある部分だけが暗号化され、各データ・フレームの暗号化のデータは、該データ・フレームの前記ヘッダ・フィールドで伝送されるのが最も好ましいことを特徴とする請求項1から14のいずれか一項に記載の方法。

【請求項16】 データ通信システムのデータ転送機器（MS，SGSN）間で転送された情報の暗号化手段、

前記情報の一つ以上のデータ・パケットを形成する手段、及び前記データ・パケットのデータ・フレームを形成する手段を備えているデータ通信システムにおいて、前記情報の暗号化手段は、

- 暗号化キー（Kc）によりデータ・パケットを暗号化する手段、
- データ・フレームに同期データ（COUNT）を配属する手段、
- 各データ・フレームの前記伝送で前記同期データ（COUNT）の前記値を変える手段、及び
- レシーバ側の前記データ転送機器において同期データを解釈する手段を少なくとも備えていることを特徴とするデータ通信システム。

【請求項17】 前記データ転送手段は、少なくとも一つの移動局（MS）を備えていることを特徴とする請求項16に記載のデータ通信システム。

【請求項18】 前記データ転送手段は、少なくとも一つの基地局（BTS）を備えていることを特徴とする請求項16に記載のデータ通信システム。

【請求項19】 前記移動局（MS）は、GSM移動局であることを特徴とする請求項17に記載のデータ通信システム。

【請求項20】 前記基地局（BTS）は、GSM基地局であることを特徴とする請求項18に記載のデータ通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、少なくともヘッダ・フィールド及びデータ・フィールドを備えている一つ以上のデータ・フレームがアプリケーションにより情報から形成された一つ以上のデータ・パケットから形成されるデータ通信システムにおけるデータ通信機器間で転送される情報の暗号化方法に関する。更に本発明は、データ転送機器間で転送される情報の暗号化手段、情報から一つ以上のデータ・パケットを形成する手段及びデータ・パケットからデータ・フレームを形成する手段を備えているデータ通信システムに関する。

【0002】

【従来の技術】別個のデータ転送機器間のデータ転送は、それらの間でそのときのデータが転送されるべきそれらのデータ転送機器がデータ転送に必要な時間の間互いに結合されるような方法で達成することができる。この場合、その結合は、ユーザがデータ転送を停止するまで維持される。そのような場合には、結合時間のほとんどの部分は、ユーザによって供給されるコマンドを入力することに費やされかつ時間のほんの少しの部分が実際のデータ転送である。これは、例えば、同時ユーザの最大数を制限する。別の可能性は、いわゆるパケット切替えデータ伝送を利用することである。この場合には、データは、パケット・モードにおいてデータ転送機器間で

転送され、そのような場合には、パケット間の時間は、自由に利用可能でありかつ他のデータ転送機器によって用いることができる。この場合には、同じセルラー・エリアにある移動局が同じ転送チャネルを用いることができるので、同時のユーザの数は、特にセルラー・ネットワークのような、無線データ転送ネットワークにおいて、増大することができる。一つのそのようなセルラー・システムは、パケット・モードデータ転送サービスGPRS（ジェネラル・パケット・ラジオ・サービス）が開発されたGSM（グループ・スペシャル・モバイル）システムである。図1は、GPRSシステムの動作における主要ブロックのブロック図を示す。パケット・スイッチング・コントローラSGSN（サービングGPRSサポート・ノード）は、セルラー・ネットワーク側のパケット・スイッチング・サービスの動作を制御する。パケット・スイッチング・コントローラSGSNは、移動局MSのサイン・オン及びサイン・オフ、移動局MSの位置の更新及びそれらの正しい宛先へのデータ・パケットのルーティングを制御する。移動局MSは、無線インターフェイスUmを通して基地局サブシステムBSSに接続される（図1）。基地局サブシステムは、BSS-SGSNインターフェイスGbを通してパケット・スイッチング・コントローラSGSNに接続される。基地局サブシステムBSSでは、基地局BTS及び基地局コントローラBSCは、BTS-BSCインターフェイスAbisによって相互に接続されている。移動局ネットワークにおけるパケット・スイッチング・コントローラSGSNの位置は、例えば、どの技術的実現（インプリメンテーション）が用いられるかにより変えることができる。図1では、パケット・スイッチング・コントローラSGSNが基地局サブシステムBSSの外側に示されているが、パケット・スイッチング・コントローラSGSNは、例えば、基地局サブシステムBSSに接続される基地局BTSの一部または基地局コントローラBSCの一部として設けることができる。

【0003】GPRSシステムは、例えば、本発明の出願日以前の日付を有する草案GSM01.60、GSM02.60、GSM03.60及びGSM04.60に記載されている。移動局MS及びパケット・スイッチング・コントローラSGSNの両方の動作は、図2に示したように、それぞれが異なる機能を提供している種々の層に分割することができる。国際標準化機構、ISOは、データ転送を異なる機能層にグループ化するためのOSI（オープン・システム・インターコネクション）モデルを公式化した。このモデルでは、全てのデータ通信システムにおいて必ずしも必要ではない7つの層がある。

【0004】移動局MSとパケット・スイッチング・コントローラSGSNの間で、ユーザによって伝送されたデータ及び制御信号のような、転送可能情報は、データ

・フレーム・モードで交換されるのが好ましい。各層のデータ・フレームは、ヘッダ・フィールド及びデータ・フィールドからなる。図2は、また、異なる層のGPRSシステムに用いられているデータ・フレームの構造を示す。

【0005】データ・フィールドに含まれた情報は、例えば、移動局のユーザによって入力されたデータまたは信号データでよい。データ・フィールドは、無線経路にそれを伝送する前にできるだけ確実に保護されなければならない機密情報を含みうる。そのような場合には、暗号化は、パケット・スイッチング・コントローラSGSNとそれに接続された移動局MSとの間の全ての同時接続において、個別の暗号化キーが用いられるような方法で実行されなければならない。逆に言えば、移動局MSは、共有無線経路資源を用いるので、即ち、多くの異なる接続における情報が同じチャネルで、例えば、異なる時間間隔で、転送されるので、データ・フィールドの暗号化に用いられたのと同じ暗号化キーによってデータ・フレームのアドレス・データを暗号化することは、好ましくない。この場合には、各移動局は、関係しているチャネルで伝送された全てのメッセージを受信しかつメッセージが向けられた移動局を識別するために少なくともアドレス・データの暗号化を暗号解読すべきである。また、パケット・スイッチング・コントローラSGSNは、どの暗号化キーを用いるべきか分からない。

【0006】次に、GPRSシステムの層の動作機能を示す。最下位層は、パケットを伝送しかつ受信するためのチャネルを割り当てることのような、移動局MSと基地局サブシステムBSSの間の通信における無線経路の使用を制御するMAC（メディア・アクセス・コントロール）層と呼ばれる。最下位レベルにおけるパケット・コントローラSGSNと基地局サブシステムの間のデータ伝送は、標準Q.921によるLAPDプロトコル、フレーム・リレー・プロトコルまたは同等物のような、リンク層プロトコルが用いられる、L2層（リンク層）で実行される。L2層は、GPRS仕様による品質またはルーティング・データも更に含みうる。層L2は、OSIモデルの物理層及びリンク層の特性を有する。基地局サブシステムBSSとパケット・コントローラSGSNの間の物理伝送回線は、例えば、パケット・コントローラSGSNがシステムにおいて配置された場所に依存する。

【0007】MAC層の上に、RLC層（ラジオ・リンク・コントロール）があり、その機能は、無線経路へ伝送すべく固定された大きさのパケットにLLC層によって形成されたデータ・フレームを分割すること及び必要であればそれらの伝送及び再伝送である。GPRSシステムにおけるパケットの長さは、1GSMタイム・スロットの長さ（おおよそ0.577ms）である。

【0008】LLC（ロジック・リンク・コントロー

ル）層は、移動局MSとパケット・コントローラSGSNの間に信頼できる伝送リンクを提供する。LLC層は、例えば、誤り検査データを伝送されたメッセージに加え、それにより、それらの不正確に受信されたメッセージを訂正しようとし、必要なときには、メッセージは、再伝送することができる。

【0009】SNDC層（サブネットワーク・ディペンデント・コンバージェンス）は、伝送された情報のプロトコル変換、圧縮、セグメンテーション及び上部層からくるメッセージのセグメンテーションのような機能を備えている。更に、暗号化及び暗号解除は、SNDC層で達成される。SNDCフレームの構造も図2に示されている。SNDCフレームは、SNDCヘッダ・フィールド（SNDCヘッダ）及びSNDCデータ・フィールド（SNDCデータ）を備えている。SNDCヘッダ・フィールドは、プロトコル・データ（ネットワーク・レイヤー・サービス・アクセス・ポイント・アイデンティティ、NLSI）及び、圧縮、セグメンテーション及び暗号化の決定のような、SNDC制御データからなる。SNDC層は、上部レベルで用いられるプロトコルとLLC層（リンク層）のプロトコルの間のプロトコル・アダプタとして機能する。

【0010】伝送された情報は、GPRSシステムによるメッセージまたはインターネット・プロトコル（IP）のパケットのような、あるアプリケーションからSNDC層へデータ・パケットとしてやってくるのが好ましい。アプリケーションは、例えば、移動局のデータ・アプリケーション、テレコピー・アプリケーション、移動局へのデータ伝送リンクを有するコンピュータ・プログラム、等であることができる。

【0011】MAC層、RLC層、LLC層及びL2層は、OSIモデルの層2で記述される特性を含む。上記した層及びOSIモデルで記述された層は、しかしながら、明確な一貫性がない。SNDCフレームは、LLCヘッダ・フィールドがフレームに加えられるLLC層へ転送される。LLCヘッダ・フィールドは、テンポラリ・ロジカル・リンク・アイデンティティ（TL LI）及びLLC制御部分からなる。パケット・コントローラGPRSは、移動局MSとパケット・コントローラGPRSの間の各データ伝送リンクに対するTL LI識別子（アイデンティティ）を確立する。このデータは、どのデータ伝送リンクに各メッセージが属するかを画定するためのデータ伝送で用いられる。同時に、同じTL LI識別子は、一つのデータ伝送リンクにおいてのみ用いることができる。リンクの終了後、リンクで用いられたTL LI識別子は、その後形成される新しいリンクへ割り当てられることができる。LLC制御部分は、誤り無しデータの転送を確実にするためのフレーム番号及びコマンド型（インフォ(info)、肯定応答、再伝送要求、等）を規定する。

【0012】GSMシステムにおける暗号化は、ビット毎の暗号化として物理層で実行される、即ち、無線経路へ伝送されたビット・ストリームは、暗号化キーK_cを用いて、本質的に知られたアルゴリズムA₅を用いて形成される伝送されたデータ暗号化ビットへ加えることによって形成される。アルゴリズムA₅は、データ転送に割り当てられたチャネルの物理層で伝送されたデータ及び信号情報を暗号化する（トラフィック・チャネル、TCHまたはデディケイテッド・コントロール・チャネル、DCCH）。

【0013】伝送されたメッセージの同期は、アルゴリズムA₅が特別な同期データ（COUNT）により駆動されるような方法で確保される。同期データCOUNTは、TDMAフレーム番号に基づき形成される。次いで、アルゴリズムA₅によって形成された各114ビット・ブロックの内容は、フレーム番号及び暗号化キーK_cにのみ依存する。

【0014】暗号化キーK_cの設定は、割り当てられたチャネルの通信トラフィックがまだ暗号化されておらずかつ用いられている移動局ネットワークが移動局MSを識別したときの段階で実行されるのが最も好ましい。GSMシステムにおける識別では、移動局を識別しかつ移動局に記憶されている、インターナショナル・モバイル・サブスクライバ・アイデンティティ、IMSIが用いられるか、または、加入者識別子に基づき形成されている、テンポラリ・モバイル・サブスクライバ・アイデンティティ、TMSIが用いられる。移動局では、また、加入者識別キー、K_iが記憶されている。加入者識別キーK_iは、また、移動局ネットワークによっても知られている。

【0015】暗号化キーK_cが移動局MS及び移動局ネットワークによってのみ知られるということを確実にするために、基地局サブシステムBSSから移動局MSへの暗号化キーの伝送は、間接的である。次いで、基地局サブシステムBSSでは、移動局MSへ伝送されるランダム・アクセス・ナンバー、RANDが形成される。暗号化キーK_cは、図3に示したような、アルゴリズムA₈を用いて、ランダム・アクセス・ナンバーRANDから及び加入者識別キーK_iから形成される。暗号化キーK_cの計算及び記憶は、移動局MS及び移動局ネットワークの両方で実行される。

【0016】移動局MSと基地局サブシステムBSSの間のデータ転送は、接続の開始では暗号化されない。暗号化されたモードへの遷移は、基地局サブシステムBSSが、ここでは“スタート・サイファ（start cipher）”と呼ばれるある一定のコマンド（暗号化されていない）を移動局へ伝送するような方法で進められるのが好ましい。移動局MSがコマンド“スタート・サイファ”を受信した後、それは、伝送されたメッセージの暗号化及び受信したメッセージの暗号解読を開始する。そ

れに対応して、基地局サブシステムBSSは、基地局サブシステムが移動局によって伝送された暗号化されたメッセージを受信しかつ正しく暗号を暗号解読した後に、移動局へ伝送されるメッセージの暗号化を開始する。

【0017】

【発明が解決しようとする課題】上述した暗号化では、同期は、例えば、物理層のTDMAフレーム番号に基づいていた。全てのアプリケーションにおいて、特に、パケット切替えデータ伝送方法におけるような、異なる接続（コネクション（connection））に属する情報が同じチャネルで伝送されるときに、それを用いることができない。

【0018】欧州特許EP-0689316号公報では、例えば、暗号化キーを備えている暗号化データが伝送されたデータ・フレームに配属（アタッチ（attach））されるような、データ転送の暗号化に対する方法が示されている。米国特許US-5,319,712号公報は、リンク層のデータ・フレームにシーケンス番号が配属されかつデータ・フレームが暗号化されるようなデータ転送の暗号化に対する方法及び装置を備えている。従来技術によるこれらの暗号化方法の欠点は、例えば、受信者が、暗号解読することなしでは、受信したデータ・フレームが誰に向けられたものかが分からず、不必要なデータ・フレームの受信及び暗号解読がシステムの効率における低下をもたらす。

【0019】本発明の目的は、転送されたデータがデータ・フレーム・モードにありかつデータ転送システムがデータ・フレーム構造が異なる層において異なることができるような機能層に分割されているデータ転送システムにおけるデータ転送の暗号化方法及び装置を提供することである。

【0020】

【課題を解決するための手段】本発明による方法は、データ・パケットの少なくともある部分が暗号化キーによって暗号化され、かつ同期データがデータ・フレームに配属され、かつその値が少なくとも各データ・フレームの伝送で変更されることを特徴とする。本発明によるシステムは、情報を暗号化する手段が少なくとも

- データ・パケットを暗号化キーで暗号化する手段、
- 同期データをデータ・フレームに配属する手段、
- 各データ・フレームの伝送で同期データの値を変更する手段、及び
- 受信者のデータ転送機器における同期データを解釈する手段を備えていることを特徴とする。

【0021】従来技術による暗号化方法と比較して、相当な利点が本発明によって達成される。本発明による方法では、物理層のデータ・フレームのヘッダ・フィールドは、暗号化されていないモードで伝送することができるか、または現在知られている方法を暗号化に用いることができる。本発明の好ましい実施例による方法では、

暗号化キーは、物理層の各伝送ブロックに対して変更され、暗号化キーについての知識なしで暗号解読することは、実質的に不可能である。本発明による方法を用いることによって、部分的暗号化を実現することが更に可能であり、伝送されたデータ・フレームの一部だけが暗号化される。この場合には、例えば、広告が暗号化されないままに送付されかつ暗号化されたデータ・フレームを受信しかつそれらを暗号解読する権利を有するものに対してだけ他の情報が暗号化されて送付されることができ

【0022】

【発明の実施の形態】本発明は、添付した図面を参照して以下により詳細に説明される。以下において、本発明は、GSMシステムで実現されたパケット切替えサービスGPRSにより具体化されているが、しかしながら、本発明は、このシステムだけに限定されるものではない。

【0023】本発明では、例えば、GPRSシステムにおける、データ・フレームの伝送にそれが適用できるように調整されるGSMシステムの暗号化のような、できるだけ多くの既存の暗号化技術が利用されるインプリメンテーションを目的にしている。本発明の一つの利点は、ポイント間接続（PTP（ポイントツーポイント）接続）、多重ポイント接続（PTM-M（ポイントツーマルチポイントマルチキャスト）；PTM-G（ポイントツーマルチポイントグループ））、その他、等のような、多くの動作モードにそれを適用することができるということである。暗号化方法は、TLLI識別子に基づき主に分類される。明確なTLLI識別子は、移動局MSとパケット・スイッチング・コントローラSGSNの間の各接続型に対して割り当てられる。以下の異なる型は、本標準によるGPRSシステムにおける使用に対して利用可能である：

— ポイントツーポイント（PTP）は、移動局MSとパケット・スイッチング・コントローラSGSNの間の通信に独自のTLLI識別子を用いる。

【0024】— ポイントツーマルチポイントマルチキャスト（PTM-M）は、移動局MSとマルチキャスト・サービス・プロバイダの間の通信に対して割り当てられたTLLIを用いる。

— ポイントツーマルチポイントグループ（PTM-G）は、移動局グループ内の移動局MSのマルチキャスト・サービス・プロバイダを介して相互通信に対して割り当てられたTLLIを用いる。

【0025】ポイントツーポイント接続は、リンク層レベルで肯定応答モードを一般に用いる、即ち、伝送のレシーバ（受信器）は、正しい受信の肯定応答としてデータを伝送する。ポイントツーマルチポイント接続では、データ・フレームは、肯定応答が伝送されない動作モードを用いて通常伝送される。この説明において

既に先に示したように、異なる接続（コネクション(connection)）のデータが同じチャネルで伝送されるシステムでは、各接続に対して独自の暗号化キーによってデータ・フレームのヘッダ・フィールドを暗号化するのは好ましくない。この場合には、データ・フレームは、物理層以外の他の層で少なくとも部分的に暗号化される。GPRSシステムでは、暗号化は、LLC層で実行される。伝送されたデータは、データ・フレームの各ビットに対して、暗号化ビット・ストリングの対応ビットが合計されるような方法で暗号化される。暗号化ビット・ストリングは、個別かつ独自の暗号化キーKcを用いて暗号化アルゴリズムによって形成されているのが好ましい。暗号化アルゴリズムは、例えば、GSMシステムから知られたA5アルゴリズムである。

【0026】正しいアドレスに加えて、データ・フレームがレシーバ（受信器）でシーケンス化することができることを確実にしなければならない。これは、既に知られた方法で実現することができ、同期データCOUNT（カウント）は、暗号化アルゴリズムに入力され、レシーバが、暗号解読後に、データ・フレームのシーケンスを見出すことができる。例えば、TDMA（タイム・ディビジョン・マルチプル・アクセス(Time Division Multiple Access)）システムでは、GSMのように、物理層のデータ・フレームに番号を付けるためにTDMAフレーム番号を用いることができる。しかしながら、GPRSシステムのパケット・スイッチング・コントローラSGSNは、TDMAフレーム番号を知らず、そこでこの発明ではデータ・フレームを同期するための方法が開発され、この方法でデータ・フレームのシーケンス番号（データ・フレーム番号）が同期データとして用いられる。それゆえに、各伝送されたブロックの内容は、例えば、フレーム番号及び暗号化キーKcによって決定される。

【0027】暗号化されるべきデータの量は、異なる接続において変わるが、暗号化が伝送されたデータを好ましくは標準長さのサブブロックに分割することによって実行できるので、これは、本発明のアプリケーションにおいて重要ではない。次いで、各サブブロックの第1のビットが暗号化アルゴリズムの第1のビットによって、サブブロックの第2のビットが暗号化アルゴリズムの第2のビットによって等、暗号化される。GPRSシステムでは、サブブロックの長さは、例えば、本GSMシステムにおけるような、114ビットでありうる。好ましくは、サブブロックの長さは、また、バイトの長さにより分割可能でもありうる。多くのアプリケーションでは、バイトの長さは、8であり、サブブロックに対する適切な長さは、64ビットでありうる。

【0028】GSMシステムでは、移動局MSは、一度に一つの暗号化キーKcだけを用いることができる。GPRSシステムでは、移動局は、各接続が異なる手段に

10

20

30

40

50

よって形成されているのが好ましい個別の暗号化キーKcを有しているのが最も好ましい多くの異なる型のアクティブ接続(PTP, PTM)を同時に有することができるので、移動局MS毎に一つの暗号化キーは、全ての状況において必ずしも十分ではない。それゆえに、暗号化されたデータ・フレームは、用いられた暗号化キーKc、同期データCOUNT及び可能であればまたTLIに配属されたブロック・カウンタBLCNTの値COUNTb(カウントb)を含む。図4は、暗号化されていないサブブロック(プレイン・テキスト・イン)がネットワークから移動局へ暗号化されて(暗号化されたテキスト)転送される状況における略ブロック図として本発明による好ましい暗号化方法を示す。この実施例では、また、ブロック・カウンタの値COUNTbは、暗号化ブロックBLOCK1の決定において用いられる。ブロック・カウンタは、好ましくは各適応層のデータ・フレームの開始において、設定ライン“クリア(clear)”によりその初期値に設定することができる。ネットワーク側及び移動局MSの両方において、同期データCOUNTの値は、暗号化アルゴリズムA5に入力された同期データCOUNTの値及び暗号化キーKcで、各伝送されたブロックについて計算される。伝送側では、出力ビット・ストリング(BLOCK1(ブロック1))は、サブブロック(プレイン・テキスト・イン)に加算される。暗号化されたサブブロックは、移動局MSへチャネル内を転送される。移動局MSは、受信した暗号化サブブロックと暗号化アルゴリズムA5の出力ビット・ストリング(BLOCK1)とを加算することによってそれ相応にそれを暗号解読し、加算結果として、伝送されたサブブロックに対応している未だ暗号化していないサブブロック(プレイン・テキスト・アウト)が得られる。図5は、略ブロック図として本発明による別の好ましい暗号化方法を示す。この実施例は、主にブロック・カウンタBLCNTが用いられていないということにおいて図4の実施例とは異なる。

【0029】フレーム・シーケンス番号の一般的な長さは、6から8ビットである。暗号化機密の観点から、COUNT変数としてのこの値だけでは十分でなく、従って、また、フレーム・シーケンス番号、例えば、基地局識別子に加えて他の変数を同期データのCOUNT値の決定に用いることができる。使用中の移動局が基地局の変更についてパケット・スイッチング・コントローラSGSNに知らせるので、基地局識別子は、ネットワーク及び移動局の両方によって知られている。それゆえに、基地局の変更によりこの実施例における同期データのCOUNT値が変わる。

【0030】ポイントツーポイント接続モードでは、次の値は、同期データのCOUNT値の決定において利用可能である：

a) 適応層(SNDC)に運ばれるロジカル・リンク・

コントロール(LogicalLink Control)層のフレーム番号(LLCフレーム番号、LLC#)。

b) それが接続の両端で維持されるときに接続の開始で初期化されるかまたは伝送されたデータ・フレームに配属されることができる適応層のデータ・フレーム番号(SNDCデータ・ブロック番号、SDN#)。

【0031】c) 識別子が伝送されたデータ・フレームに配属される必要がないように接続の両端で知られるルーティング・エリアの識別子(ルーティング・エリア#)。

d) 識別子が伝送されたデータ・フレームに配属される必要がないように接続の両端で知られるパケット・スイッチング・コントローラのエリアの識別子(SGSN#)。

【0032】e) 識別子が伝送されたデータ・フレームに配属される必要がないように接続の両端で知られる基地局の識別子(Cell#)。ポイントツーマルチポイント接続モードでは、次の値は、同期データのCOUNT値の決定において利用可能である：

a) SNDCデータ・フレーム内に伝送される適応層のデータ・フレーム番号(SNDCデータ・ブロック番号、SDU#)

b) 識別子が伝送されたデータ・フレームに配属される必要がないように接続の両端で知られるルーティング・エリアの識別子(ルーティング・エリア#)。

【0033】c) 識別子が伝送されたデータ・フレームに配属される必要がないように接続の両端で知られるパケット・スイッチング・コントローラのエリアの識別子(SGSN#)。

d) 識別子が伝送されたデータ・フレームに配属される必要がないように接続の両端で知られる基地局の識別子(Cell#)。

【0034】更に、両方の接続モードにおいて、同じ暗号化ビット・ストリングがシーケンシャル・データ・フィールドの暗号化で用いられないので、ブロック・カウンタBLCNTの値を用いることができ、侵入者にとって、暗号化されたデータ・フィールドのクラッキングをさらに困難にする。さもなければ、再計算が適応層のデータ・フレームの各伝送に対して一度だけ実行される。適応層のデータ・フレームの長さは、数千ビットでありうるし、暗号化アルゴリズムが十分に何度も計算されないならば暗号化キーを見出すことが可能でありうる。

【0035】同期データCOUNTを定義している上記変数は、単独または組合せのいずれかで用いることができる。それゆえに変数のあるものは、データ・フレーム内のレシーバへ送付されなければならないしかつそれらのあるものは、局所的に管理することができる。局所的に管理される変数の使用は、機密のレベルを増大しかつある程度までそれは、転送されたデータの量を低減する。次の表は、同期データCOUNTのコンテンツの例

を示す。表1. 1は、本発明の最も好ましい実施例による同期データを示しかつその中に、ブロック・カウンタBLCNTが用いられ、かつ表1. 2は、本発明の別の好ましい実施例を示しかつその中に、基地局の識別子が*

表1. 1

ビット /モード	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
PTP	SDU # (ローカル又は配送した)								LLC # (配送した)						COUNTb							
PTM	SDU # (配送した)								1	1	1	1	1	1	COUNTb							

【0037】

【表2】

表1. 2

ビット /モード	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
PTP	SDU # (ローカル又は配送した)								LLC # (配送した)						セル#, ルーティング・エリア#, 又はSGSN # (ローカル)							
PTM	SDU # (配送した)								1	1	1	1	1	1	セル#, ルーティング・エリア#, 又はSGSN # (ローカル)							

【0038】次に、暗号化キーKcの設定を説明する。暗号化キーKcの設定は、ネットワーク・オペレータがそれを必要とする度にネットワークによって起動される。更に、独自の暗号化キーが各TLLI接続に対して生成されなければならない。暗号化キーKc-TLLI識別子ペアの表は、パケット・スイッチング・コントローラSGSN及び移動局MSの両方に維持されるのが最も好ましい。暗号化キーの設定は、異なる接続型に対して異なる。

【0039】ポイントツーポイント接続では、暗号化キーKcは、ランダム・アクセス番号RANDを用いて間接的に伝送される。暗号化キーKcは、ちょうどGSMシステムにおけるように、アルゴリズムA8を用いて好ましくはランダム・アクセス番号RANDから及び移動局の加入者識別キーKiからGPRSシステムで形成される。移動局の識別キーは、移動局のSIM (サブスクライバ・アイデンティティ・モジュール(Subscriber Identity Module)) カード及びネットワークのオーセンティケーション・センターAuCに記憶されている。

【0040】マルチポイント接続では、同じサービスに接続される全ての移動局は、同じ暗号化キーKcを用いる。暗号化キーKcは、サービスへの接続が生成されるときに起動される。暗号化キーKcは、異なる方法を用いて移動局MSに入力することができる。マルチポイント・サービス・プロバイダは、例えば、暗号化されたモードで、暗号化キーを入力することができ、移動局MSは、マルチポイント接続へのアクセスを得る前にポイントツーポイント接続を通してパケット・スイッチング・コントローラSGSNにログされなければなら

*ブロック・カウンタCOUNTbの値の代わりに用いられている。

【0036】

【表1】

い。ポイントツーポイント接続のログオン段階中に、暗号化キーKcは、接続に対して定義されかつ、それは、それが移動局MSへ伝送されるときにマルチポイント接続の暗号化キーの暗号化に用いられる。

【0041】マルチポイント接続の暗号化キーは、また、例えば、PINコード、のような、移動局MSのキーパッドを用いて、入力することができるか、または一種のSIMカードは、他のパラメータの中で、暗号化キーKcが記憶されているところで用いることができる。暗号化キーKcは、暗号化キーを先のパケット・スイッチング・コントローラから新しいものへ送付することができるので、移動局MSが別のパケット・スイッチング・コントローラGPRSのエリアへその位置を変えるとときに再生成される必要がない。

【0042】クリア・テキスト・モードから暗号化モードへの遷移は、パケット・スイッチング・コントローラGPRSが特別な“スタート・サイファー(start cipher)” コマンドをクリア・テキストで伝送するような方法で進行するのが好ましい。移動局MSでは、移動局によって“スタート・サイファー” コマンドが正しく受信された後に伝送の暗号化及び受信の暗号解読が開始する。パケット・スイッチング・コントローラGPRS側では、暗号化は、パケット・スイッチング・コントローラが移動局MSによって伝送されたメッセージを受信しかつそれを暗号解読した後にそれ相応に開始する。上記動作は、その主な部分において、GSMシステムの暗号化の開始に対応する。

【0043】あるパケット・スイッチング・アプリケーションでは、暗号化は、また、一方向へ行くメッセー

ジ、即ち、移動局MSからパケット・スイッチング・コントローラGPRSへのまたはパケット・スイッチング・コントローラGPRSから移動局MSへのメッセージだけが暗号化されるような方法で適用することができる。このようなアプリケーションは、例えば、通常は、暗号されないで伝送される広告の送付を含む。

【0044】更に、本発明による暗号化は、適応層SND Cの伝送されたデータ・フレームのある部分だけが暗号化されるような方法で適用することもできる。この場合には、一つの暗号化ビットが適応層のデータ・フレームに加えられるのが最も好ましくかつそれは、考慮するデータ・フレームが暗号化されるかまたは暗号化されていないかを示す。例えば、暗号化ビットが値ゼロを有するとき、データ・フレームは、暗号化されておらず、暗号化ビットが値1を有するとき、データ・フレームは、暗号化されている。これは、例えば、サービスへのアクセス権利が登録または同等物を必要とするような状況において、用いることができ、登録されたユーザは、暗号化されたデータ・フレームを暗号解読することができる。他のユーザに対して、サービス・プロバイダは、暗号化されていないデータ・フレームのサービス及び広告に関する情報を送付することができる。

【0045】図6の(a)は、好ましい実施例によるリンク層のデータ・フレーム構造の例を示す。データ・フレームのヘッダ・フィールド(フレーム・ヘッダ)は、3バイトのTL L I識別子及び2バイトの制御部分(コントロール(Control))を含む。バイトは、既に知られているように、8つの2進情報(ビット)を含む。データ・フレームの情報フィールドは、伝送された情報を含む。情報フィールドの長さは、変わりうる。データ・フレームは、また、例えば、誤り訂正情報を含む2バイトの検査フィールド(チェック・シーケンス(Check sequence))を含む。

【0046】図6の(b)は、データ・フレームが情報送付及びシステム・スーパーバイザリ・データ・フレーム(インフォメーション+スーパーバイザリ(information+ supervisory))であるときの図6の(a)のデータ・フレームの制御部分の構造を示し、その中で、C/Rは、それがコマンドまたは応答の質問(コマンド/レスポンス(Command/Response))であるかどうかを示す、S1及びS2は、スーパーバイザリ・コマンドの型を記述し、N(S)は、送信順序の番号(送信順序番号(Send sequence number))であり、P/Fは、それが確認要求メッセージ(P)または確認メッセージ(F)の質問であるかどうかを示し、(ポル/ファイナル(Poll/Final))、そしてN(R)は、受信順序の番号(受信順序番号(Receive sequence number))である。

【0047】図6の(c)は、データ・フレームがシステム・スーパーバイザリ・データ・フレーム(スーパーバイザリ(Supervisory))であるときの図6の(a)のデ

ータ・フレームの制御部分の構造を示す。ビットの意味は、上述した。図6の(d)は、データ・フレームが番号なしデータ・フレーム(アンナンバード(Unnumbered))のときの図6の(a)のデータ・フレームの制御部分の構造を示し、その中で、M1-5は、番号なしコマンド及び応答であり、G/Dは、それが制御またはデータ・フレームの質問であることを示し(コントロール/データ(Control/Data))、そしてx-ビットは、重要でない。

【0048】図7は、好ましい実施例による適応層のポイントツーポイント接続を有するデータ・フレーム構造の例を示す。第1のバイトは制御データを含み、その中で、

- Mは、それがアプリケーションによって形成された情報の最後のセグメントの質問であるかどうかを示し、
- Eは、暗号化が使用中であるかどうかを示し、
- Priは、優先分類(priority classification)を示し、
- NLSIは、例えば、
- TCP/IP、
- CLNP、
- X.25、
- GPRS、等

であるような、プロトコル・データを示す。

【0049】図8は、好ましい実施例による適応層のマルチポイント接続を有するデータ・フレーム構造の例を示す。ビットの意味は、上述した。本発明は、移動局MS、基地局サブシステムBSS及びGPRSシステムのパケット・スイッチング・コントローラSGSNが用いられるデータ転送システムで上述したが、本発明は、パケット・スイッチング・データ転送システムにおいて最も好ましい、TDMA及びCDMAデータ転送システムのような、他のデータ転送システムにも適用することができる。

【0050】本発明は、上記実施例にのみ限定されず、それは、特許請求の範囲の範囲内で変更することができる。

【図面の簡単な説明】

【図1】GPRSシステムのロジック構造を示す略ブロック図である。

【図2】GPRSシステムの層構造及び層のデータ・フレーム構造を示す図である。

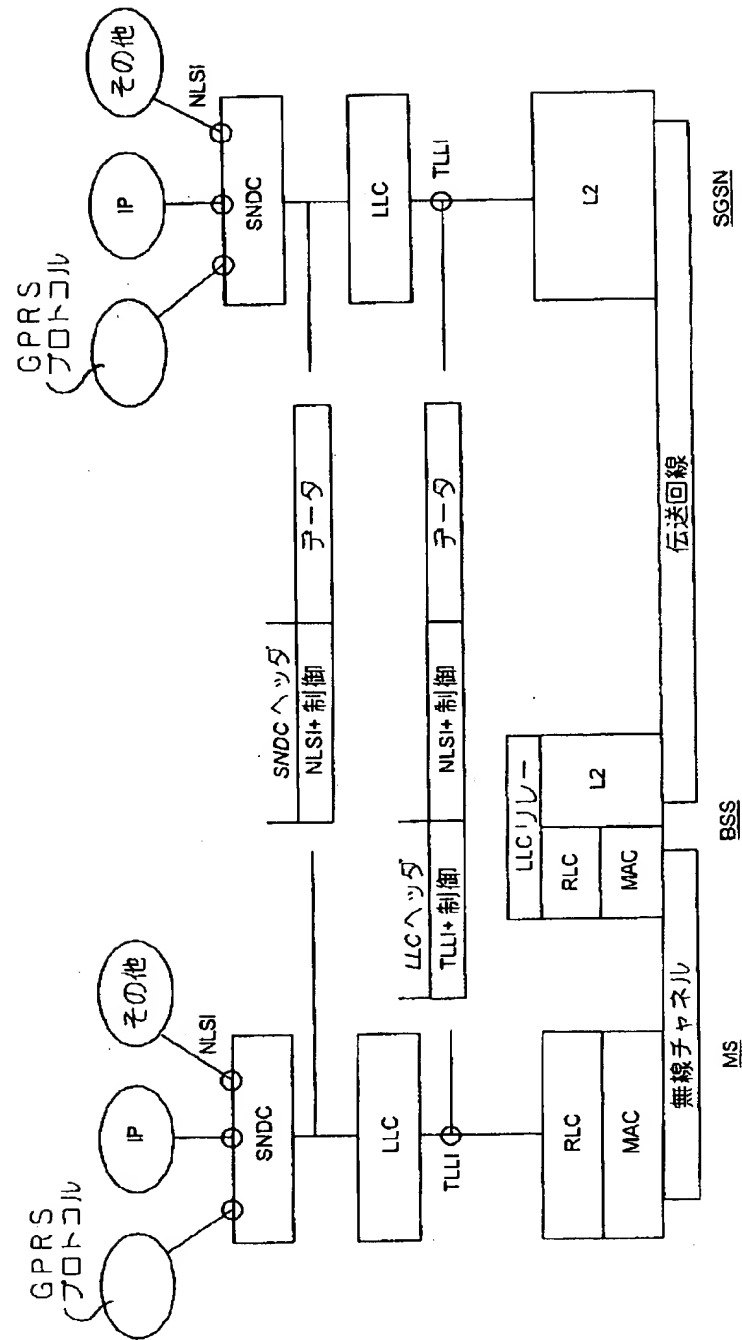
【図3】移動局及び移動局ネットワークにおける従来技術による暗号化キーの定義を示す略ブロック図である。

【図4】本発明の好ましい実施例による暗号化を示す図である。

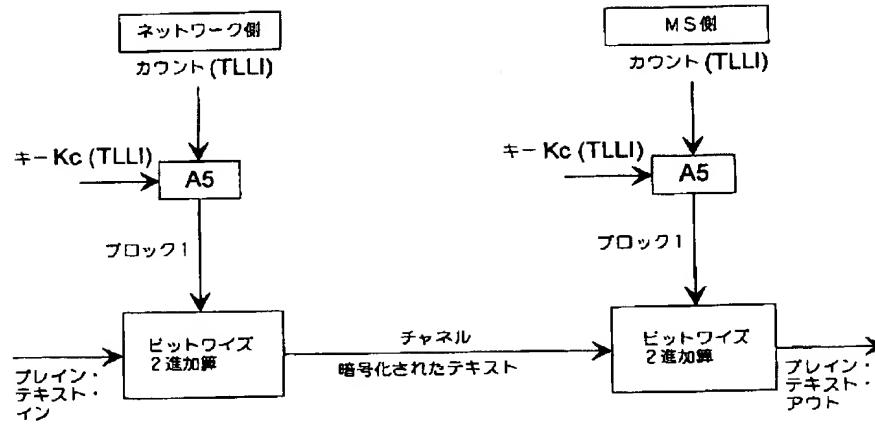
【図5】本発明の別の好ましい実施例による暗号化を示す図である。

【図6】実施例によるリンク層のデータ・フレーム構造を示す図である。

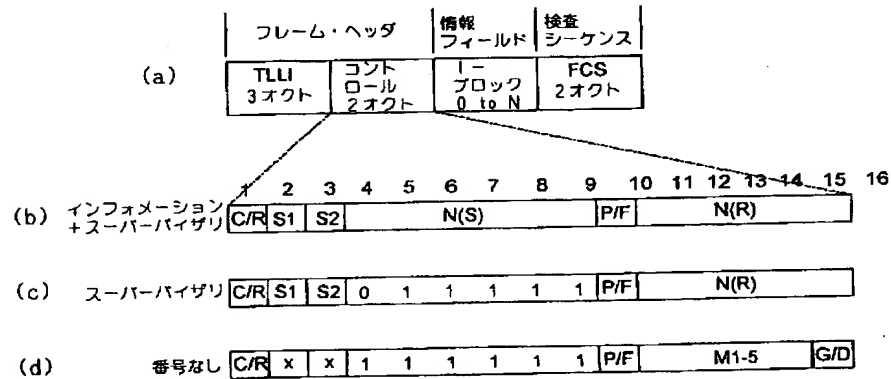
【図2】



【図5】



【図6】



【図8】

ビット	8	7	6	5	4	3	2	1
オクト1	M	E	Pri		NLSI			
2	SDU番号							
...	データ・セグメント							
N								

フロントページの続き

(72)発明者 ヤリ ヘーメーレイネン
フィンランド国、エフイーエン-33720
タンペレ、マティ タピオンカトゥ 1
エフ 17

(72)発明者 ヤリ ユオッペイ
フィンランド国、エフイーエン-00410
ヘルシンキ、ルートナンティンティエ 3
デー 30